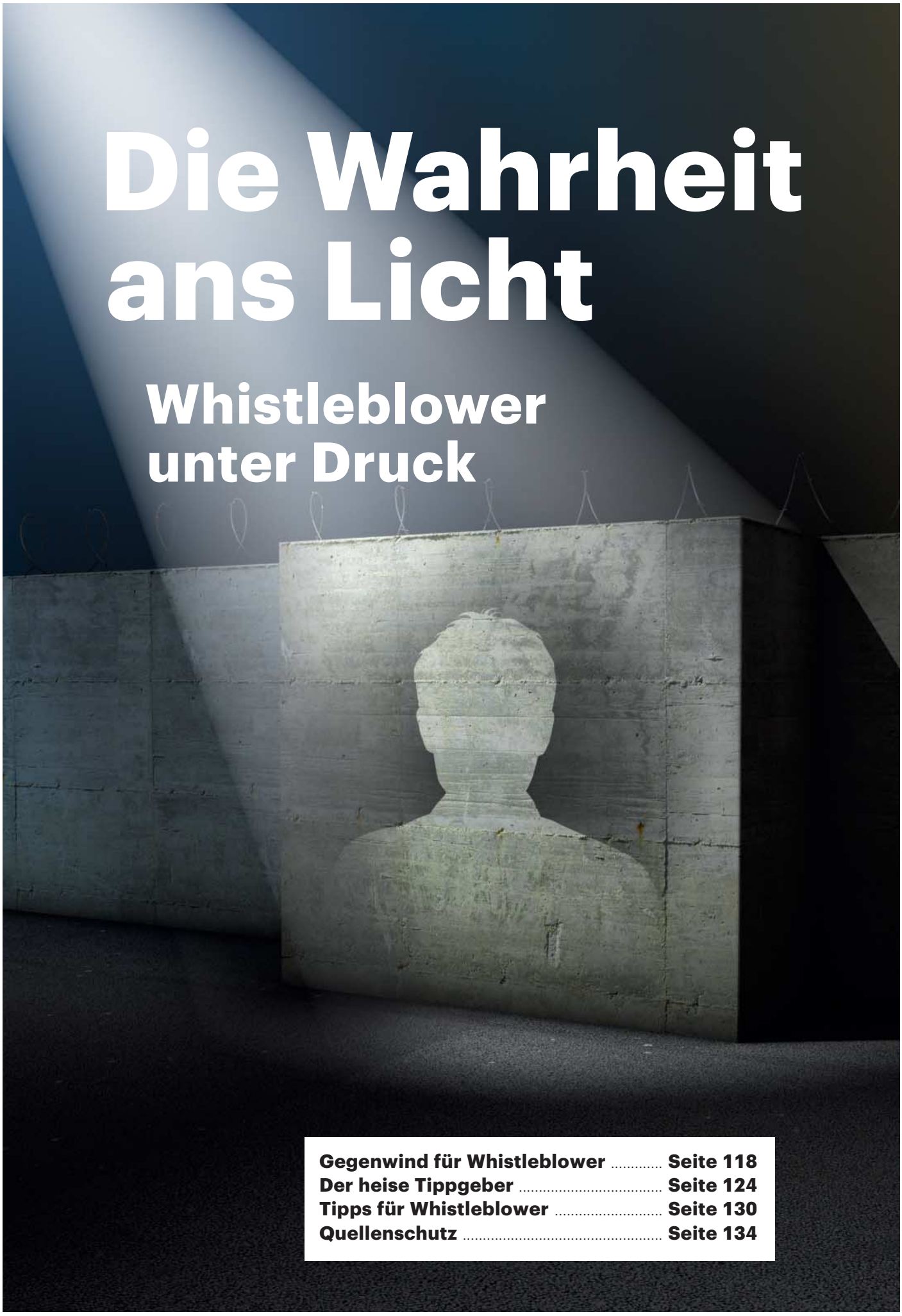
Die Wahrheit ans Licht

Whistleblower unter Druck



Mutige Mitarbeiter von Unternehmen und Behörden, die mit Informationen über Missstände an die Öffentlichkeit gehen, werden von den Mächtigen gehasst und gefürchtet. Die Auseinandersetzung darum, wie man mit Informationen und Informanten umgehen soll, wird mit harten Bandagen geführt.

Von Detlef Borchers

Auf der ganzen Welt gibt es Whistleblower, Lanceurs d'Alerte, Reveladors de Secretos, die Klokkenluider, Visselblåsare und Fløjteblæser, Hinweisgeber und ethische Dissidenten. Sie bringen aus Behörden, Firmen oder Organisation heraus geheime Missstände an die Öffentlichkeit. Sie wollen die Missstände damit abstellen oder wenigstens eine gesellschaftliche Debatte darüber in Gang setzen.

Oft haben sie damit Erfolg: Mit den Panama Papers im April dieses Jahres befeuerte ein bislang Unbekannter die Debatte über die Kluft zwischen Arm und Reich, mit den NSA-Dokumenten brachte Edward Snowden die umfassende Überwachung durch die National Security Agency ans Licht. Chelsea Manning verbüßt derzeit eine 35-jährige Freiheitsstrafe. Sie machte das Grauen des Krieges greifbar, indem sie vertrauliches Material über Feldzüge und Gefangenenlager der USA veröffentlichte.

Whistleblower wenden sich an Zeitungen oder an einzelne Journalisten, wenn sie die Öffentlichkeit suchen. Vormals geheime Dokumente kann man aber nicht einfach auf irgendeinen Server hochladen. Wer sie veröffentlicht, muss sie auswerten, verifizieren, Recherchen dazu vornehmen und Beteiligte durch Schwärzungen schützen. Etablierte Medien leisten dabei gute Dienste. Sie haben die dafür notwendigen Fachleute wie Redakteure und Juristen und einen großen Leser- oder Zuschauerstamm, der für die nötige Aufmerksamkeit sorgt.

Für die Mächtigen sind die Whistleblower alles andere als einsame Helden, die gegen Missstände kämpfen. Sie zeichnen lieber das Bild des Verräters und berufen sich auf rechtliche Regelungen zum Schutz von Geheimnissen. Betroffene Firmen und Behörden setzen oft alles daran, den Whistleblower zu enttarnen und anschließend zu diskreditieren. Das schafft ein Klima der Angst, das hohe Hürden für Geheimnisträger schafft, sich zu offenbaren.

Das bekannteste aktuelle Beispiel ist der US-Amerikaner Edward Snowden. Er hätte die internen Meldewege benutzen müssen, um die von ihm ans Licht gebrachten Missstände abzustellen, behauptet die Präsidentschafts-Anwärterin Hillary Clinton noch heute. Dass diese Meldewege nicht funktionierten, ignoriert sie dabei.

Snowden entschloss sich zum Gang an die Öffentlichkeit, obwohl er als Angestellter eines Dienstleisters nicht den Schutz des Whistleblower Protection Act in den USA genießt. Und selbst der steht nur auf dem Papier: Snowden verfolgte, wie hochrangige IT-Spezialisten der National Security Agency (NSA) vom FBI belangt wurden, obwohl ihnen Schutz zugesichert worden war. Er setzte sich deshalb ins Ausland ab und suchte von dort aus den Kontakt zu unabhängigen Journalisten. Letztlich landete er in Russland, wo er bis heute im Exil lebt.

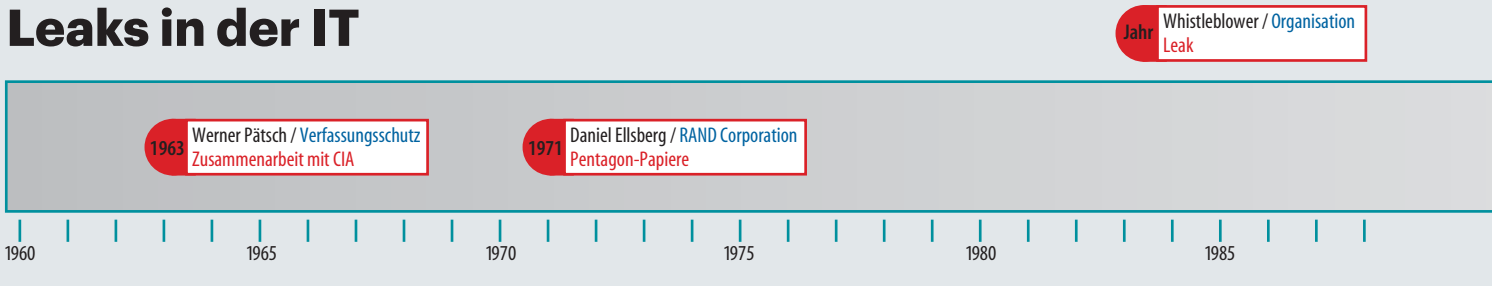
Wer wie Snowden in der IT-Branche arbeitet, hat oftmals weitreichenden Zugriff auf brisante Daten. Nur Fachleute können beispielsweise bemerken, wenn Suchläufe in Datenbanksystemen mittels „Selektoren" so eingestellt sind, dass sie gegen gesetzliche Auflagen verstoßen. Snowden war zuletzt als Angestellter von Booz Allen Hamilton im First Level Support für die Mitarbeiter der NSA tätig und konnte als Außenstehender dennoch Tausende von Dokumenten über die Arbeit der NSA sammeln. Prompt wurde er von manchen Medien als „Hacker" bezeichnet – zu Unrecht. Hackern geht es um IT-Schwachstellen, die sie zum Guten oder zum Schlechten ausnutzen.

Ein neues Wort

Whistleblower standen schon immer unter Beschuss. Das erste Mal wurde der Begriff auf einer Konferenz verwendet, die der US-amerikanische Verbraucherschutzanwalt Ralph Nader 1970 veranstaltete. Er prägte ihn, um ihn positiv zu besetzen und negativ besetzten Begriffen wie Verräter oder Informanten entgegenzustellen. Im IT-Bereich wurde die Idee in der ethischen Diskussion schnell aufgegriffen: Im Jahre 1970 veröffentlichte die einflussreiche British Computer Society erstmals ihren „Code of Conduct". Er gilt als der älteste Verhaltenskodex der Informatiker überhaupt.

Mit 42 Richtlinien sollte der ethisch verantwortungsvolle Umgang mit Computern geregelt und das korrekte Verhalten von Programmierern und Systemadministratoren beziehungsweise Operatoren festgelegt werden. Im New Scientist kritisierte der Sozialwissenschaftler Joseph Hanlon den Kodex scharf: „[Er] enthält Geheimnis-Klauseln, die das Whistleblowing im Stil von Nader verhindern sollen, mit dem die Öffentlichkeit über schädliche Praktiken informiert wird". Whistleblower sollten durch verbindliche Richtlinien daran gehindert werden, mit der weithin hörbaren Bobbypfeife die Öffentlichkeit zu warnen, wenn sie Ungereimtheiten entdecken und sich lieber vertraulich an den Arbeitgeber wenden. Hanlon ging das je-

Leaks in der IT



doch nicht weit genug: „Nirgendwo in diesem Kodex ist davon die Rede, dass Computer-Professionals eine größere Verantwortung haben, nicht gegenüber ihrem Arbeitgeber, sondern gegenüber der Gesellschaft, wenn Programme und Computer-Systeme schädlich sind oder so genutzt werden, dass sie gesellschaftlichen Schaden anrichten."

Mit diesem Widerspruch lebt die Informationstechnologie bis heute. Dabei begann die Geschichte der Whistleblower viel früher: Werner Pätsch war Anfang der 60er-Jahre des vergangenen Jahrhunderts „Fallführer", also Sachbearbeiter, beim Verfassungsschutz und stieß bei seiner Arbeit auf streng geheime Vordrucke, mit denen die Behörde Kopier- und Abhöraktionen gegen Bundesbürger bei den alliierten Geheimdiensten der Briten und US-Amerikaner „in Auftrag" gab. Die Kollegen vom CIA erledigten dann umstandslos das, was den deutschen Staatsschützern verboten war.

Pätsch machte die Skandalpraxis der reibungslosen Zusammenarbeit der Schnüffeldienste öffentlich, indem er im Sommer 1963 zunächst einen Anwalt kontaktierte, der wiederum die Presse informierte. „Spiegel" und „Stern" berichteten, ein „Panorama"-Interview mit ihm wurde gedreht – und verschwand prompt im Giftschrank. Politiker gaben sich ahnungslos und hatten von nichts gewusst. Ein geflügeltes Wort wurde die Antwort auf die Frage, ob die Beamten des Verfassungsschutzes nicht gegen die Verfassung verstießen, die der damalige Innenminister Hermann Höcherl (CSU) gab: „Die Beamten können nicht den ganzen Tag mit dem Grundgesetz unter dem Arm herumlaufen."

Bild:Laura Poitras/Praxis Films, CC BY 3.0 https://creativecommons.org/licenses/by/3.0

Der Whistleblower Edward Snowden lebt heute auf der Flucht vor den US-Strafverfolgungsbehörden im Exil in Russland.

1965 wurde Pätsch angeklagt, Staatsgeheimnisse verraten und damit das Wohl der BRD aufs Spiel gesetzt zu haben. Im Prozess vor dem Bundesgerichtshof ging es um die Frage, ob der Verrat des Staatsgeheimnisses strafbar ist, wenn das Staatsgeheimnis selbst eine verfassungswidrige Praxis ist. Der BGH fällte eine weitreichende Entscheidung: „Es gibt deshalb einen Kernbereich des Verfassungsrechts, bei dessen Verletzung jeder das Recht haben muss, sofort und ohne jeden Umweg die Öffentlichkeit anzurufen, auch wenn dies zwingend zur Preisgabe von Staats- oder Amtsgeheimnissen führt." Der „ethische Dissident" Pätsch wurde nur dafür verurteilt, beim Aufdecken der verfassungswidrigen Praxis den Dienstweg nicht eingehalten zu haben. Bis heute dürfen die alten Akten zum Fall Pätsch auf Weisung des Verfassungsschutzes nicht eingesehen werden, „da aus dem Akteninhalt auf konkrete, noch heute relevante Arbeitsweisen und Organisationseinheiten des Bundesamtes für Verfassungsschutz geschlossen werden kann."

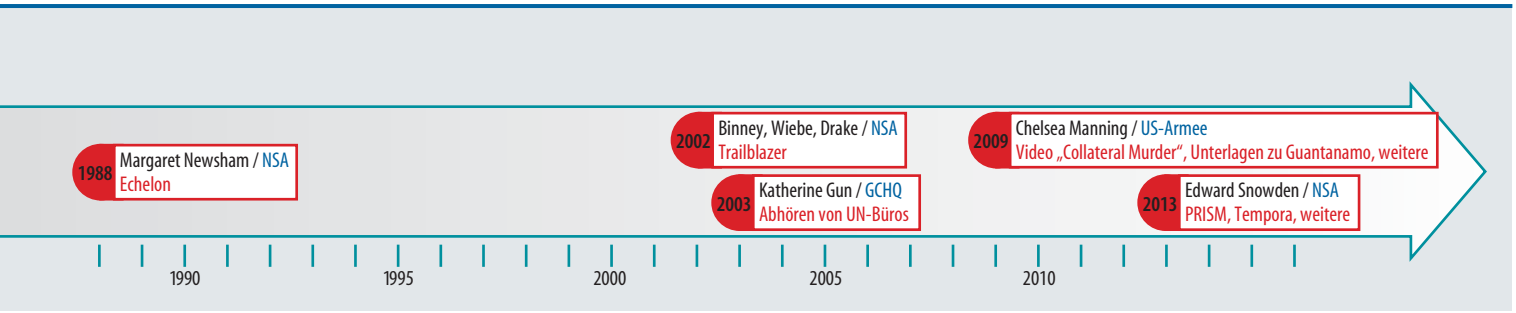
Mal eben 7000 Seiten kopieren

Daniel Ellsberg ist der berühmteste Whistleblower des vergangenen Jahrhunderts. Die von ihm im Sommer 1971 vervielfältigten 7000 Seiten der „Pentagon-Papiere" dokumentierten das Ausmaß der systematischen Desinformation, mit der die US-Regierung unter Präsident Nixon das Land hinsichtlich des Vietnamkriegs täuschte. Für Ellsberg war es schwierig, die zögernden Journalisten der New York Times und Washington Post von der Veröffentlichung zu überzeugen.

Auch der später angestrengte Prozess gegen Ellsberg ist historisch bedeutsam. Die Richter des US Supreme Courts urteilten ähnlich wie die deutschen Richter im Fall Pätsch, dass das Interesse der Öffentlichkeit und die Pressefreiheit Vorrang vor der Geheimhaltung haben können. In einem Sondervotum hieß es: „Und über allen Verantwortlichkeiten einer freien Presse steht die Pflicht, jeglichen Teil der Regierung daran zu hindern, die Menschen zu betrügen und in ferne Länder zu schicken, um an fremdländischen Krankheiten und fremdländischen Kugeln und Granaten zu sterben." Historisch ist noch ein anderer Aspekt der Pentagon Papers: Was Ellsberg und seine Kinder in mühseliger, tagelanger Arbeit kopierten, ist nur ein winziger Bruchteil der Datenmenge, die Chelsea Manning an einem Nachmittag auf eine CD brannte, die sie mit „Lady Gaga" beschriftete und hinausschmuggelte.

Auch die Existenz des Abhörsystems Echelon gelangte durch einen gezielten Geheimnisverrat an die Öffentlichkeit: 1978 wurde Margaret Newsham von ihrem US-amerikanischen Arbeitgeber im Auftrag der NSA als Systemadministratorin nach Menwith Hall in Großbritannien geschickt. Dort betreute sie bis 1984 eine Batterie von VAX-Rechnern. Sie waren als sogenannte „Dictionaries" im Einsatz, durchsuchten den zuvor von Übersetzern transkribierten Strom belauschter Telefonate und Fernschreiben der Intelsat-4-Satelliten nach Kennworten. Insgesamt bestand das P415 genannte System aus 20 Bodenstationen und 53 „Dictionaries". „Irgendwann habe ich mich gefragt, was ich hier eigentlich mache", verriet Margaret Newsham einem dänischen Reporter, der die unter einem Decknamen lebende Rentnerin in Nevada ausfindig gemacht hatte.

Als Newsham sich 1988 dem britischen Journalisten Duncan Campbell anvertraute, wurde das System mit dem



Code-Namen „Echelon“ bekannt. Ihr war bei der Arbeit in Menwith Hall aufgefallen, dass die Übersetzer Gespräche mithörten und keine Rücksicht darauf nahmen, ob etwa Amerikaner an der Kommunikation beteiligt waren. So konnte sie beispielsweise ein Gespräch verfolgen, das der republikanische Senator Strom Thurmond führte.

Die Argumentation ihrer Kollegen, dass die verfassungsmäßigen Rechte von US-Bürgern in der Zentrale in Maryland schon beachtet würden, wollte ihr nicht einleuchten. Dank der von Newsham angestoßenen Recherche von Campbell und Kollegen wie dem Neuseeländer Nicki Hager konnte das weltweit aufgespannte Echelon-System Stück für Stück enttarnt werden, auch in Deutschland, wo die US-Amerikaner eine Bodenstation in Bad Aibling betrieben. Als der deutsche BND dort das Abhören übernahm, wählte er den schönen Decknamen Hortensie für die Station.

Eine E-Mail mit Folgen

Nicht immer muss ein IT-geprägter Mitarbeiter mit Einblick in das Gesamtsystem zum Whistleblower werden. Manchmal reicht eine einzige E-Mail, wie im Jahr 2003, als die beim GCHQ arbeitende Mandarin-Übersetzerin Katherine Gun eine Mail erhielt, in der ein Vorgesetzter um Amtshilfe beim Abhören der Vereinten Nationen bat. Alles, was die damals im UN-Sicherheitsrat vertretenen Länder Angola, Bulgarien, Kamerun, Chile, Guinea und Pakistan von ihren UN-Büros mit der Heimat kommunizierten, sollte daraufhin analysiert werden, ob sich verwertbare Informationen für die Rechtfertigung eines Angriffskrieges im Irak finden ließen. Über einen Bekannten ließ die Kriegsgegnerin Gun die ausgedruckte Mail dem „Observer“ zukommen, der sie veröffentlichte. Gun, die sich einem Vorgesetzten anvertraute, wurde vom GCHQ entlassen. Der gegen sie angestrengte Prozess platz-

te, weil das GCHQ sich weigerte, den E-Mail-Verkehr freizugeben. Er enthalte Informationen, die die Arbeit des Nachrichtendienstes nachhaltig schädigen würden, eine Argumentation, die an den Fall des Whistleblowers Pätsch erinnert.

Komplizierter ist der Fall der Whistleblower William Binney, J. Kirk Wiebe, Edward Loomis, Diane Roark und Thomas A. Drake und des Whistleblower-Schützers John Crane kurz nach der Jahrtausendwende. Binney, Wiebe und Drake waren anerkannte Software-Spezialisten, die an vielen NSA-Projekten gearbeitet hatten. Auslöser ihres erst internen, später öffentlich gemachten Whistleblowings war ein neues, umfassendes Überwachungsprogramm mit dem Codenamen „Trailblazer“, das der damalige NSA-Direktor Michael Hayden für 3,8 Milliarden Dollar in Auftrag gegeben hatte. Das System sollte Unmengen an Rohdaten zur späteren Auswertung sammeln, auch Daten US-amerikanischer Bürger, was in den USA nach dem vierten Verfassungszusatz verboten ist. Datensparsamer war das unter der Leitung von Binney intern bei der NSA entwickelte „Thin Thread“, das Daten von US-Bürgern ausfilterte. Den Zuschlag bekam aber „Trailblazer“, das bis 2006 entwickelt und dann wegen erwiesener Unbrauchbarkeit eingestellt wurde. Im September 2002 beschwerten sich Binney, Wiebe und Loomis erstmals beim Generalinspekteur des Verteidigungsministeriums, ohne Erfolg.

William Binney wurde für seine Enthüllungen über das NSA-Programm „Trailblazer“ mit dem Sam Award 2015 ausgezeichnet.

Den Dienstweg einhalten

Thomas A. Drake, ein Deutschland-Spezialist der NSA, wandte sich zunächst getrennt vom Vorstoß von Binney & Co an den Generalinspekteur der NSA. Später nahm er Kontakt mit der 2001 eingerichteten Whistleblower-Anlaufstelle des Verteidigungsministeriums auf. Außerdem bat er Diane Roark um Unterstützung, eine Mitarbeiterin des „House Intelligence Committees“, das die Arbeit der Geheimdienste überwacht. Als Software-Tester in der Abteilung für Qualitätssicherung wollte Drake ausdrücklich den Dienstweg einhalten und seine Bedenken zu „Trailblazer“ vortragen.

Drake bekam die Zusage von John Crane, dem Sachbearbeiter der Whistleblower-Abteilung im Pentagon, dass seine Beschwerde vertraulich behandelt werde. Cranes Vorgesetzter informierte jedoch FBI und NSA über den Fall und schickte nach Protesten von Crane diesen selbst in den Ruhestand. Im Juli 2007 stürmten FBI-Agenten mit gezogener Waffe die Wohnungen von Binney, Wiebe, Loomis, Roark und Drake. Bei Drake, der versucht hatte, die Baltimore Sun zu informieren, wurden als geheim eingestufte Dokumente gefunden. Nach einer Anklage wegen Geheimnisverrats und Materialübergabe an die „New York Times“ drohten Drake viele Jahre Haft, doch dann wurde 2011 die Anklage reduziert auf „Zweckentfremdung eines Computersystems“, für die Drake eine einjährige Bewährungsstrafe bekam. Er verlor Haus, Ehefrau und Vermögen und gewann insgeheim einen Freund: Drakes Schicksal wurde von Edward Snowden beobachtet und analysiert. Er lernte, wie man es nicht als Whistleblower machen sollte.

Zapfstelle Wikileaks

Im Jahre 2008 betrat Wikileaks mit einem neuen Konzept die Bühne: Whistleblower sollten ihre Dokumente an Wikileaks übergeben. Die Organisation will dann entweder mit der Presse zusammenarbeiten oder selbst die Informationen aufbereiten und veröffentlichen. Durch das Zwischenschalten der Plattform sollte das Risiko einer Enttarnung der Whistleblower minimiert werden. Den größten Erfolg mit diesem Angebot hatte Wikileaks im Jahre 2010, als man ein Video aus dem Irak-Krieg unter dem Titel „Collateral Murder“ veröffentlichte. Geliefert hatte es, zusammen mit dem umfangreichen Material der „Kriegstagebücher“, ein Gefreiter der US-Armee, der als Nachrichtenanalyst arbeitete.

Chelsea Manning kopierte im Irak das ihr zugängliche umfangreiche Material auf eine CD, die sie wie eine selbstgebrannte Musik-CD beschriftete und mit nach Hause nehmen konnte. Als Wikileaks das Material bekam und begann, es in Zusammenarbeit mit Zeitungen wie dem Guardian und dem Spiegel zu veröffentlichen, war Mannings Mission bereits erfüllt. Zum Verhängnis wurde ihr, dass sie sich in einem Chat gegenüber einem FBI-Informanten ihrer Tat rühmte. 2013 wurde Manning zu einer Haftstrafe von 35 Jahren verurteilt.

Nicht jeder Whistleblower muss sich am Ende zwangsläufig vor Gericht rechtfertigen oder gar eine Haftstrafe verbüßen. Wer bei der Veröffentlichung anonym agiert oder einen vertrauenswürdigen und kompetenten Partner wählt, kann auch aus der Deckung heraus agieren. Was dabei zu beachten ist und welche Strategien Erfolg versprechen, lesen Sie in den Artikeln auf den folgenden Seiten.

(uma@ct.de) c't